



# HID: prodikeys: Check presence of pm->input\_ep82

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-43251
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-06 12:16:45 UTC
<b>Updated</b>	2026-05-11 18:51:22 UTC
<b>Description</b>	In the Linux kernel, the following vulnerability has been resolved: HID: prodikeys: Check presence of pm->input_ep82 Fake

## Risk And Classification

**Primary CVSS:** v3.1 5.5 MEDIUM from nvd@nist.gov

**CVSS:** 3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

**Problem Types:** CWE-476

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

**CVSS:** 3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 3a370ca1dcf8c80aff7a0a21d6b0f50ca2a151e9 f580c79683356632f12f2c2029f2fe936d953aa1 git
CNA	Linux	Linux	affected 3a370ca1dcf8c80aff7a0a21d6b0f50ca2a151e9 ee572578f09f0e743e9383393a75c3a7a0f9b4c2 git
CNA	Linux	Linux	affected 3a370ca1dcf8c80aff7a0a21d6b0f50ca2a151e9 edccbf7d6dc05d692bde3a89de5a4001f72a0fa4 git
CNA	Linux	Linux	affected 3a370ca1dcf8c80aff7a0a21d6b0f50ca2a151e9 3f1b21cc67a15d7d081378a9b8747dd000a017b8 git
CNA	Linux	Linux	affected 3a370ca1dcf8c80aff7a0a21d6b0f50ca2a151e9 e7ac1cd823cd2e9fcbd5cb0b261d6d35dbb79341 git
CNA	Linux	Linux	affected 3a370ca1dcf8c80aff7a0a21d6b0f50ca2a151e9 d5512ce892f774d37c53082adadfcad04f21b50e git
CNA	Linux	Linux	affected 3a370ca1dcf8c80aff7a0a21d6b0f50ca2a151e9 d08f35f843881ec504d7537a9bb728a073db3366 git
CNA	Linux	Linux	affected 3a370ca1dcf8c80aff7a0a21d6b0f50ca2a151e9 cee8337e1bad168136aecfe6416ecd7d3aa7529a git
CNA	Linux	Linux	affected 2.6.35
CNA	Linux	Linux	unaffected 2.6.35 semver
CNA	Linux	Linux	unaffected 5.10.252 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.202 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.165 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.128 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.75 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.16 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.6 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

## References

Reference	Source	Link	Tags
git.kernel.org/stable/c/edccbf7d6dc05d692bde3a89de5a4001f72a0fa4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/f580c79683356632f12f2c2029f2fe936d953aa1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/cee8337e1bad168136aecfe6416ecd7d3aa7529a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/d08f35f843881ec504d7537a9bb728a073db3366	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/3f1b21cc67a15d7d081378a9b8747dd000a017b8	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/ee572578f09f0e743e9383393a75c3a7a0f9b4c2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/d5512ce892f774d37c53082adadfcad04f21b50e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/e7ac1cd823cd2e9fcbd5cb0b261d6d35dbb79341	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonic

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)